



Business Client Advisory Update (2009 – U2)

Issued: October 25, 2008
First Update: February 19, 2009
Second Update: August 17, 2009

On August 17, 2009, the Executive Office of Consumer Affairs & Business Regulation announced several modifications to the Massachusetts personal information security regulations in order to better balance consumer protection with the concerns of small businesses.

The revised regulations are now scheduled to take effect on March 1, 2010. Under the “risk-based” approach of the new requirements, every business will have greater flexibility to design a personal information security program that is appropriate to its size, scope and activities.

Topic: Corporate Law – Massachusetts has adopted new regulations governing the security of personal information collected by businesses.

Summary: Beginning March 1, 2010, every business that, in connection with the provision of goods and services or for purposes of employment, collects and retains personal information about a Massachusetts resident is required to adopt a written security program that is appropriate to the size, scope and resources of the business as well as the nature and volume of the personal information the business collects.

Common Questions/Practical Answers

- 1. What information qualifies as personal information?** Personal information is defined as a Massachusetts resident’s first name and last name or first initial and last name, combined with either: (a) a Social Security number; (b) a driver’s license or state identification card number; or (c) a financial, credit card or debit card account number (collectively, the above is referred to as “**Personal Information**”). Personal Information does not include any lawfully obtained information available to the general public.
- 2. Who is required to comply with these regulations?** Every person, corporation or partnership that owns, licenses, stores or maintains Personal Information about a Massachusetts resident in connection with the provision of goods and services or for purposes of employment is required to comply with these regulations. In addition, if a person, corporation or partnership electronically stores or transmits Personal Information, there are additional security requirements that must be met.
- 3. What is required of businesses governed by these regulations?** A business that falls under these regulations must develop and implement a comprehensive, written information security program for the Personal Information it stores (a “**CWISP**”). In the event that a business stores or transmits Personal Information electronically, the business must also incorporate into its CWISP certain minimum

steps, each to the extent technically feasible (that is, capable of being undertaken using reasonable means through technology), covering any computers or wireless networks that contain the Personal Information. The basic requirements of a CWISP are attached hereto. The statute giving rise to these regulations, MGL Chapter 93H, also sets forth the detailed requirements for the reporting, by a business, of any unauthorized access or use, or any other compromise to the security, confidentiality or integrity, of collected Personal Information.

4. **What is the risk to my business?** If a business is found to have an insufficient personal information security program, the Massachusetts Attorney General may bring a MGL, Chapter 93A action (a “**Chapter 93A Action**”) against that business. A Chapter 93A Action can result in an injunction against the business to prevent the collection or use of Personal Information, and/or may include the award of up to treble damages and/or attorney’s fees to an individual harmed by an unauthorized release of Personal Information. In determining whether a personal information security program is sufficient, the Attorney General will take into account: (a) the size, scope and type of business; (b) the amount of resources available to such business; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee Personal Information.

5. **What can I do to lower my risk?** The first step to lower your risk is to determine if your business stores or uses Personal Information. If that is the case, you will need to prepare a CWISP based on the attached guidelines. **Coleman & Gagnon** is preparing a questionnaire on our website that we will use to prepare a customized version of this important document for each of our clients.

6. **What should I do if I have questions?** Once you have ascertained your risk, **Coleman & Gagnon** can counsel you in determining the best CWISP for your business and assist you with implementation of the CWISP. If you have been reported to, and/or are subject to, an Attorney General action or other related litigation, **Coleman & Gagnon** can refer you to an experienced litigation attorney to represent you.

Legal Disclaimer: The content of this **Business Client Advisory** is provided for informational purposes only. It is not legal advice and should not be construed as such. Please do not act upon this information without seeking professional advice or rely on this **Business Client Advisory** or use the content as a substitute for consultation with professional advisors. Receipt of this **Business Client Advisory** by any party is not intended to and will not create an attorney/client relationship with such recipient.

IRS Circular 230 Disclosure: Please be advised that any discussion of U.S. tax matters contained within this communication (including any attachments) is not intended or written to be used and cannot be used for the purpose of avoiding U.S. tax related penalties.

About Coleman & Gagnon: **Coleman & Gagnon** is a boutique corporate law firm assisting entrepreneurs in reducing risk and avoiding circumstances that might limit their success. The firm’s attorneys pride themselves on finding creative solutions to challenging problems. We focus on advising start-up companies, providing general corporate counsel to existing companies and representing businesses in merger and acquisition transactions. Visit our website at www.colemangagnon.com for more information.

Duty to Protect and Standards for Protecting Personal Information
(201 CMR 17.03)

- (1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.
- (2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:
- (a) Designating one or more employees to maintain the comprehensive information security program;
 - (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
 - 1. ongoing employee (including temporary and contract employee) training;
 - 2. employee compliance with policies and procedures; and
 - 3. means for detecting and preventing security system failures.
 - (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
 - (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
 - (e) Preventing terminated employees from accessing records containing personal information.
 - (f) Oversee service providers, by:
 - 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
 - 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that any contract a person has entered into with a third party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.
 - (g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

- (h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- (i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Computer System Security Requirements

(201 CMR 17.04)

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (a) control of user IDs and other identifiers;
 - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - (d) restricting access to active users and active user accounts only; and
 - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
 - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.